UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,638	07/02/2002	Gregory Burdett	08894984US	7715

7590 08/22/2006

GOWLING LAFLEUR HENDERSON, LLP
Suite 2600
160 Elgin Street
Ottawa, ON K1P 1C3
CANADA

EXAMINER	
HERRING, VIRGIL A	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 08/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/774,638	BURDETT ET AL.	
	Examiner	Art Unit	
	Virgil Herring	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 June 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is responsive to the amendment filed 5 June 2006. Claims 1-11 are currently pending, of which independent claims 1 and 7 have been amended.

Response to Amendment

The amendments to the figures, specification, and claims are sufficient to overcome the prior objections. The prior objections are withdrawn.

Response to Arguments

Applicant's arguments filed 5 June 2006 have been fully considered but they are not persuasive.

With regards to applicant's argument that Chuah "does not teach or suggest establishing "an encrypted acceleration tunnel between a VPN acceleration client and a VPN acceleration server", the examiner submits that Chuah teaches wireless VPN, and that the acceleration (applicant's preferred word for "optimization") is taught by Gleeson, causing a rejection under 35 USC § 103.

With regards to applicant's assertion that Chuah "clearly teaches away from the present invention", examiner notes applicant's cite of column 9, lines 18-30. The examiner does not agree with the argument that this paragraph teaches away from the claimed invention, because it clearly indicates VPN communication using a wireless

device. Lines 31-64 and figures 8-9 indicate that the "new control messages" referenced by applicant are used in a secondary tunnel created for the handoff process while roaming, not in the main tunnel from the wireless device to the LNS 135. Examiner submits that Chuah cannot possible teach away from the claimed invention when both Chuah and the claimed invention detail the steps of establishing VPN communications between a wireless device and an enterprise network.

With regards to applicant's argument that there is no motivation to combine the teachings of Chuah and Gleeson because Chuah teaches away from the invention, examiner again points out that Chuah teaches the steps of establishing a VPN between a wireless device and a corporate network, as described above.

With regards to applicant's argument that the combination of Chuah and Gleeson relied upon in the previous office action "is fundamental different than the present claimed invention", examiner disagrees. Applicant's claimed invention is encrypted VPN using a wireless device and "acceleration", defined in the specification as optimization techniques applied in the network layer. The combination described in the last office action is VPN using a wireless device and an extra optimization layer between the network layer and data link layer in the OSI model. These are fundamentally the same concept, because in both cases, the optimization takes place at a level above the data link layer.

Claim Objections

Claims 1 and 7 are objected to because of the following informalities:

Claim 1 as amended includes extra punctuation. Specifically, there is a semicolon in line 13 and a period in line 15 which must be removed.

The new limitation added to claims 1 and 7 contains a grammatical deficiency that impedes reading the claims. The use of "utilized same" is improper, and appears that it should read "utilize the same".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chuah et al (US Patent # 6,496,491) in view of Gleeson et al (US Patent # 5,446,736).

With regards to claim 1, Chuah et al disclose a method of securely communicating customer premises equipment based virtual private network transmissions over a carrier network comprising the steps of:

establishing an encrypted tunnel between a VPN client and a VPN server in response to a VPN client request for information; (Figure 8, where connection 814 corresponds to the encrypted tunnel, wireless PC 805 corresponds to the VPN client, and serving NAS 815 corresponds to the VPN server)

transmitting said VPN client's VPN address and required data information to said VPN server over said encrypted acceleration tunnel; (inherent step required for all VPNs)

establishing an encrypted VPN tunnel between said VPN server and an appropriate VPN switch thus providing access to the appropriate enterprise content servers, said appropriate enterprise ~~Enterprise~~ content server corresponding with said required data information transmitted; (Figure 8, where connection 816 corresponds to the encrypted VPN tunnel, serving NAS 815 corresponds to the VPN server, and router 165 corresponds to the VPN switch, and the corporate network contains one or more content servers)

encrypting and transmitting required data corresponding to said required data information from said VPN switch to said VPN server over said VPN tunnel, said required data is communicated from said appropriate Enterprise content server to said VPN switch prior to encryption and transmission; (inherent, see below)

decrypting said required data at said VPN server; (inherent, see below)

encrypting by said VPN server and transmitting said required data to said VPN client; and (inherent, see below)

decrypting said required data in response to said VPN client receiving said required data. (inherent, see below)

Chuah et al do not expressly disclose the use of wireless transmission acceleration in a VPN. However, Gleeson et al disclose methods for wireless transmission optimization in both WANs and LANs.

The optimization taught by Gleeson et al takes place in an "optimization layer", inserted between the network layer and data link layer of the OSI stack. The examiner notes that this is analogous to the applicant's system, in which the "acceleration" is performed by using transmission optimization techniques in the network layer. Applicant defines acceleration as "wireless communication performance optimization techniques including compression, protocol optimization, caching, and traffic management". Gleeson et al disclose: "standard protocols are optimized by filtering and discarding some protocol packets, generating and 'synthesizing' the reception of other protocol packets, and removing and transforming protocol header fields" (Col. 3, Lines 50-56). Removing protocol header fields results in compression of the packets involved. Also, filtering and discarding some packets is clearly an example of traffic management. Additionally, Gleeson et al discuss caching of data packets (although they use the word buffer) in column 21, lines 19-22. Thus, the disclosure of Gleeson et al teaches all four factors of wireless acceleration.

At the time of the invention, it would have been obvious to those skilled in the art that the wireless WAN optimization techniques of Gleeson et al would also be applicable in the wireless VPN of Chuah et al. The motivation for this would have been to "allow the use of standardized protocols to interface wireless nodes with the wireless network while taking into account the special characteristics of the wireless WAN" (Gleeson et al, Col. 3, Lines 33-36).

Several steps of claim 1 are marked as "inherent, see below". Communications in a Virtual Private Network must necessarily be encrypted to protect the privacy of the network. Thus, the packets are inherently sent in an encrypted form from the "real" network to the serving NAS 815 on the virtual network. Because the teachings of Gleeson et al are applied to serving NAS 815, the packets must be decrypted within that device before the optimization steps can be applied. The optimized packets must then be encrypted before being sent to wireless PC 805 to maintain the privacy of the VPN. The optimized packets must then be decrypted again at wireless PC 805 before they can be used.

With regards to claim 7, the combination of Chuah et al and Gleeson et al would include a server for providing secure virtual private network service for wireless clients comprising:

a first module for terminating a virtual private network tunnel to a private network switch; (Chuah et al as modified by Gleeson et al: Figure 8, where

serving NAS 815 includes a module for establishing connection 816 through the Internet to router 165)

a second module for accelerating data for transmission over a wireless network; and (Chuah et al as modified by Gleeson et al: Figure 8, where serving NAS 815 includes a module for wireless communication optimization as described above)

a third module for terminating an encrypted tunnel to a wireless client whereby a secure virtual network service is provided between the private network service is provided between the private network and the wireless client, for which acceleration of data on the wireless network is provided. (Chuah et al as modified by Gleeson et al: Figure 8, where serving NAS 815 includes a module for establishing connection 814 to wireless PC 805)

With regards to the new limitation of claims 1 and 7 "wherein said encrypted acceleration tunnel and said VPN acceleration server utilized same network layer in a standard OSI model", examiner points out that although Gleeson depicts the "optimization layer" as an extra OSI layer, it is technically a part of the network layer. The ISO definition of the OSI layer describes the data link layer as the one that "is built upon one or several physical-connections." This is differentiated from layers 3-7, which are not disclosed as including physical components. The optimization described by Gleeson takes place above the data link layer, which implies that it is based in software, which would make it a part of the lowest software layer, namely the network layer. See

the Open Systems Interconnection – Basic Reference Model (ISO/IEC 7498-1), sections 7.1.2, 7.2.2, 7.3.2, 7.4.2, 7.5.2, 7.6.2, and 7.7.2 for a more in-depth explanation.

With regards to claims 2 and 11, the combination of Chuah et al and Gleeson et al as described above does not include a method as claimed in claim 1 wherein the step of establishing an encrypted acceleration tunnel uses public key infrastructure (PKI) encryption. However, Hagen (US Application # 2002/0075844 A1) discloses a system and method for integrated public and private network resources for optimized broadband wireless access. Specifically, in paragraph [0070], Hagen discloses the use of "conventional Internet security protocol (IPSec) ... operating with a conventional public key infrastructure (PKI) digital certificate service;" and that "as known in the art, IPSec is preferably operated in tunnel mode ... thus establishing a virtual private network (VPN)." Hagen is analogous art with the combination of Chuah et al and Gleeson et al, because his goal is optimized wireless online access (as in Gleeson et al) using VPN (as in Chuah et al). As Hagen states, the use of both IPSec and PKI are "conventional" and IPSec VPNs are "known in the art". Thus, it would have been obvious for one skilled in the art to consider both PKI and IPSec in the VPN of Chuah et al.

With regards to claim 3, the combination of Chuah et al and Gleeson et al as described above includes a method as claimed in claim 1 wherein the required data

information includes at least one of a VPN switch address, user name, and password. (Chuah et al, Col. 4, Lines 31-32; the VPN switch address is required, because the user name and password would only apply to a certain private network)

With regards to claims 4 and 8, the combination of Chuah et al and Gleeson et al, as further modified by Hagen includes a method as claimed in claim 1 wherein the encrypted VPN tunnel is an IPSec tunnel.

With regards to claims 5 and 9, the combination of Chuah et al and Gleeson et al as described above does not include a method as claimed in claim 1 wherein the encrypted VPN tunnel is an MPLS tunnel. However, Forslow (US Application # 2002/0133534 A1) discloses a network-based mobile workgroup system. Specifically, in paragraph [0020]: "Several solutions have been put forward to achieve different levels of network privacy when building VPNs across a shared IP backbone, so target network-based VPNs. Most of these solutions require separate per VPN forwarding capabilities and make use of IP or MPLS based tunnels across the backbone network." Thus, at the time of the invention it would have been obvious to one skilled in the art to use a MPLS tunnel in a VPN, as described by Forslow as prior art.

With regards to claims 6 and 10, the combination of Chuah et al and Gleeson et al as described above includes a method as claimed in claim 1 wherein the encrypted

VPN tunnel is a L2TP tunnel. (Chuah et al, Col. 3, Lines 61-67; the NAS support the L2TP)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Virgil Herring whose telephone number is (571) 272-8189. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Virgil Herring VH
Examiner
Art Unit 2132

KAMBIZ ZAND
PRIMARY EXAMINER

VH